# An Implementation of Fuzzy ART Algorithm for Detecting Anomaly Intrusion in LAN Environment

**John-Otumu A. M.**
ICT Directorate
Ambrose Alli University, Ekpoma,
Nigeria

**Ojieabu C. E.**
Dept. of Elect/Elect Engineering
Ambrose Alli University, Ekpoma,
Nigeria

**Oshoiribhor E. O.**
Dept. of Computer Science
Ambrose Alli University, Ekpoma,
Nigeria

***Abstract:*** *These days network security applications can be found everywhere due to the increasing size and number of Local Area Networks (LAN), and Internet connections. This paper critically examined several research works on techniques used in building Intrusion Detection System (IDS). We considered the Fuzzy ART technique for designing and building our proposed Anomaly Node Intrusion Detection System based on its strengths. The proposed system was tested in a production computer network, and the test results revealed that the proposed system is able to detect anomaly intrusion of nodes effectively. The system was evaluated for its effectiveness and efficiency. The evaluation results revealed the detection rate to be 99.98%, detection time to be 0.82 seconds and the false alarm rates (false positive and false negative to be 0.01%). The proposed system is highly recommended for usage in any local area network.*

Keywords: Agent, Anomaly, IDS, LAN, Profiling, Data Patterns, Network Traffic

## I INTRODUCTION

According to [1] the concept of Intrusion Detection System (IDS) was first introduced in early 1980's after the evolution of Internet.[2] Sees Intrusion Detection System (IDS) as a software application developed to monitor computer system or network activities with a view of finding malicious operations occurrence by an intruder. But the major goal of IDS is to monitor network traffic in order to detect anomalous behavior or hacking tendencies in data patterns. According to [3] Intrusion detection system also means a system for identifying any set of actions that attempt to compromise the integrity, confidentiality or availability of resources.

### Types of Intrusion Detection Systems (IDS)

Intrusion Detection Systems (IDSs) are of different types and uses different techniques [2]. Some known IDS types are as follows:

**Anomaly Based Intrusion Detection:**

Anomaly-based intrusion detection is a technique designed to monitor data pattern from network environment in order to discover data patterns that are not normal in terms of behavior by flagging them as an intrusion [4]. Research work by [5] used SNORT, a powerful open source network security tool to build and implement a new hybrid intrusion detection based system on campus. The engine was able to detect anomalies by filtering files and loading the infected files into its loader by a .conf file command. [6] Used honeypot technique to design and implement Local Area Network (LAN) based intrusion detection and alert system. Filtering of unauthorized access attempts to the LAN was executed with the nodes IP addresses and anomaly behavior is sent as an alert message to the systems administrator. The implementation shows a level of solution to intrusion detection problem for LAN though it is a static and standalone application running on Ubuntu Linux. The system is perceived to be vulnerable to attack, and also with a possible high false alarm rate based on the technique used.

**Signature-Based Intrusion Detection**

The signature based intrusion detection or misuse detection is a technique in which the dataset has a number of instances and every data therein in labeled normal or intrusive, and a machine learning algorithm is used to train the data set in line with the label attached to it [7].

**Target Monitoring**

According to [8] Target monitoring is a technique used for reporting any changes or modifications that is made to a system.

**Stealth Probes**

A Stealth probe is a technique that is used to gather and associates data in order to find attacks which has taken a long period of time [4].

The specific aim of our proposed method is to monitor and detect any anomalous intrusion in a local area network using agent approach and multi-factor profiling detection technique.

## II LITERATURE REVIEW

Many IDS techniques have been discussed in different literatures to prevent attacks in networks. The following are some reviewed literatures on IDS techniques for detection and prevention of network intrusion.

[9] Used a mixtures of 3 techniques in their propose design and development of IDS. A parametrical model is used for behavior modeling. The Bayesian classification

algorithm was used for detection, while the MIB variables used to provide the IDS with the needed information. [10] Also proposed a new intrusion detection and response model for wireless networks because of the vulnerabilities in wireless network environment. Research work by [11] provided a solution to intrusion detection in mobile ad-hoc networks using a three architectural system. The system was tested under two types of MANET routing protocols. A signature detection technique was proposed by [12] for investigating the ability for various routing protocols to facilitate intrusion detection when the attacker's signature is known. [13] used lightweight methods to detect anomaly intrusion in wireless sensor networks by reusing the already available information at various layers of a network stack. [14] Also proposed a lightweight anomaly intrusion detection scheme for wireless sensor networks. The system defined efficient and effective method for monitoring nodes in order to detect intrusion. The simulated test result shows the method is accurate in detecting attacks. [15] Also researched in the same area of IDS by proposing a new game theoretical architecture to analyze the interactions between pairs of attacking and defending nodes using a hybrid Bayesian technique for detection in which a lightweight monitoring system is used to estimate opponent's actions and a heavyweight monitoring system acts as a last resort of defense.

[16] Proposed an efficient agent-based anomaly intrusion detection system for ad-hoc networks. They incorporated agent technology and data mining techniques to prevent anomaly intrusion in mobile ad-hoc networks. The proposed IDS according to [16] was able to stop all successful attacks in an ad-hoc network and reduced the level of false alarm positive to barest minimum.

[17] Proposed a cooperative and distributed method for detecting intrusion in wireless ad-hoc networks. They performed experiment that was able to detect anomaly in participating multiple mobile nodes, while [18] proposed a hybrid method for detecting intrusion using Markov chain-based approach and a Hotelling's T2 test based approach to construct the local IDS for MANET.

[19] Presented a new intrusion detection system called Distributed Intrusion Detection using Mobile Agent in LAN Environment (DIDMALE). The approach used mobile agent to add mobility features to the IDS in order to gather information from attacked nodes. The IDS application reduced network bandwidth usage and increases scalability and flexibility in decentralizing data analysis.

[20] used distributed soft computing approach for designing intrusion detection system with central analyzer and controller as the heart and soul of the distributed intrusion detection system (DIDS), while [21] designed a multi-level and secured agent-based intrusion detection system using a combination of lower level detection (LLD) and upper level detection (ULD) agents to gather and analyze patterns from the network environment in order to detect network intrusion using modified Apriori algorithm.

[22] Proposed a distributed intrusion detection system using aglet mobile agent technology for monitoring and securing a heterogeneous computer network environment. The system provides advanced network monitoring, incident analysis, and instant attack data, thereby reduces network bandwidth usage, location of intrusion data and flexibility in IDS over traditional forms.

[23] designed a distributed intrusion detection system to detect attacks or security threats on computer networks using sensor based mobile agent technology. The IDS mechanism is designed for a signature-based multi-layer system, while [24] designed an agent-based intrusion detection software prototype with several anomaly detection techniques integrated by means of collective trust modeling within group collaborative detective agents for installation in a high-speed backbone networks. The agent-based IDS is based on traffic statistics in Netflow format acquired by a dedicated hardware network interface cards.

Mobile agents has the ability of overcoming latency in computer networks, reducing overload in networks, fault tolerance, system scalability, and can operate very well in heterogeneous network environment; hence it is very suitable for proffering solutions to intrusion detection problems in heterogeneous environments [25].

Researchers in the field of intrusion detection system such as [26, 27, 28, 29, 30, and 31] also used mobile agent technology to deploy various forms of intrusion detection systems for distributed and heterogeneous network environment.

## III METHODOLOGY

We proposed the Fuzzy Adaptive Resonance Theory (ART) technique for detecting anomaly intrusion in a local area network.

Fuzzy ART is a member of the ART neural network family [32]. It incorporates computations from fuzzy set theory [33] into the ART 1 neural network. It is capable of fast stable unsupervised category learning and pattern recognition in response to arbitrary input sequences.

Fuzzy ART clusters input vectors into patterns based on two separate distance criteria, match and choice. For input vector X and pattern j, the match function is defined by

$$S_j(X) = \frac{|X \wedge Wj|}{|X|} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Where $W_j$ is the weight vector associated with pattern j.

The fuzzy AND operator ∧ is defined by

$$(X \wedge Y)_i \equiv \min(xi, yi) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

and the norm j |.| is defined by

$$|X| \equiv \sum_i \; |Xi| \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3)$$

The choice function is defined by

$$T_j(X) = \frac{|X \wedge Wj|}{\alpha + |Wj|} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (4)$$

Where $\alpha$is a small constant.

For each input vector X, Fuzzy ART assigns it to the pattern j that maximizes Tj (X) while satisfying Sj(X)≥ $\rho$, where $\rho$ is the vigilance parameter,

The weight vector Wj is then updated according to

$W^{(new)}_{j} = \beta\ (X \wedge W_j^{(old)}) + (1 - \beta)W_j^{(old)}$, ………. (5)

Where $\beta$ is the learning rate parameter, $0 \geq \beta \leq 1$. If no such pattern can be found, a new pattern node is created. This procedure is illustrated in Figure 1

In order to avoid the pattern proliferation problem, Fuzzy ART uses a complement coding technique to normalize the inputs. The complement of vector X, is denoted by $X^c$, is defined by

$(X_c)_i \equiv 1 - X_i$ ……………………..…………. (6)

For an n-dimensional original input X, the complemented coded input $X^{|}$ to the Fuzzy ART system is the 2n-dimensional vector.

$X^{!} = (X, X^c) \equiv (x_1, x_2, \ldots, x_n, x^c{}_1, x^c{}_2, \ldots, x^c{}_n)$ ….. (7)

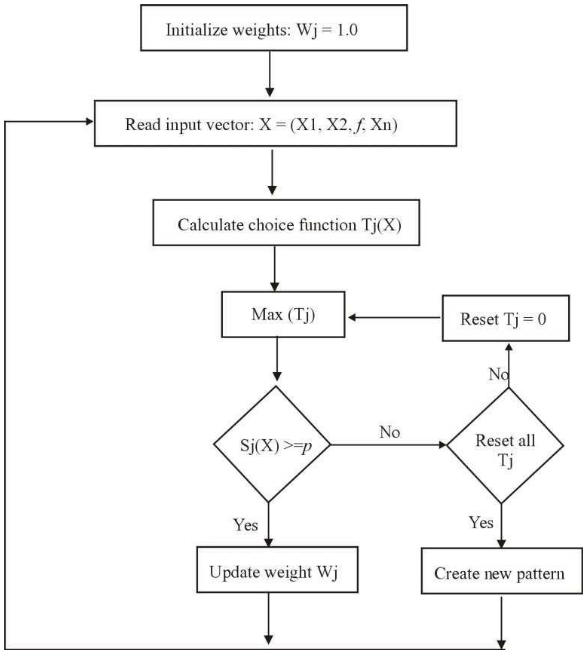
Initialize weights: Wj = 1.0
Read input vector: X = (X1, X2, *f*, Xn)
Calculate choice function Tj(X)
Max (Tj)
Reset Tj = 0
No
Sj(X) >=*p*
No
Reset all Tj
Yes
Yes
Update weight Wj
Create new pattern

Figure 1: Flowchart representation of the Fuzzy ART algorithm

Here, our proposed anomaly intrusion detection mechanism using the Fuzzy ART is trained to learn as follows:

The input vector is any personal computer system that can communicate on a local area network having the following features:

(a) node name
(b) ip address
(c) mac address
(d) system name

The vigilance parameter ($\rho$) is the features of the computer system listed above that have certain patterns to be observed, and the threshold value is the total character length of the features.

The Fuzzy system uses minimum and maximum threshold values to create a flexible detection rate.

The minimum threshold value is derived as follows. The character length for each input vector is fixed and added together to get the total character length set for the input vector (x).

node name = “node01” i.e. [6 characters]
ip address = “1.1.1.1” i.e. [7 characters]
mac address = “00.00.00.00.00.00” i.e. [17 characters]
system name = “system-01” i.e. [9 characters]
choice function = total length of input (x) = [6+7+17+9] = 39
The minimum threshold value = 39;

While the maximum threshold value is also derived as follows. The character length for each input vector is fixed and added together to get the total character length set for the input vector (x).

node name = “node500” i.e. [7 characters]
ip address = “255.255.255.255” i.e. [15 characters]
mac address = “00.00.00.00.00.00” i.e. [17 characters]
system name = “system-500” i.e. [10 characters]
choice function = total length of input (x) = [7+15+17+10] = 49
The maximum threshold value = 49

Therefore, our learning rate parameter for classifying the network traffic pattern to as normal is set as follows: $39 \leq \beta \leq 49$, otherwise anything outside this range is classified as an anomaly intrusion.

Table 1: Sample LAN profiled data for training the detection mechanism

| S/N | Node Name | System Name | MAC Address | IP Address |
|---|---|---|---|---|
| 1 | Node01 | SYSTEM-01 | D8-9D-67-CE-67-36 | 192.168.1.101 |
| 2 | Node02 | SYSTEM-02 | 08-62-66-52-FC-AF | 192.168.1.102 |
| 3 | Node03 | SYSTEM-03 | 10-1F-74-5B-B5-08 | 192.168.1.103 |
| 4 | Node04 | SYSTEM-04 | 00-03-0D-59-0D-67 | 192.168.1.104 |
| 5 | Node05 | SYSTEM-05 | C4-D9-87-30-ED-DA | 192.168.1.105 |
| 6 | Node06 | SYSTEM-06 | 01-02-0C-52-0D-17 | 192.168.1.106 |
| 7 | Node07 | SYSTEM-07 | 00-01-0D-51-0C-27 | 192.168.1.107 |
| 8 | Node08 | SYSTEM-08 | 01-03-0D-19-0A-66 | 192.168.1.108 |
| 9 | Node09 | SYSTEM-09 | 10-00-0D-59-0C-67 | 192.168.1.109 |
| 10 | Node10 | SYSTEM-10 | 00-03-0A-39-1D-47 | 192.168.1.110 |
| 11 | Node11 | SYSTEM-11 | 00-11-0C-52-0C-57 | 192.168.1.111 |
| 12 | Node12 | SYSTEM-12 | 00-0A-0A-5A-0A-60 | 192.168.1.112 |

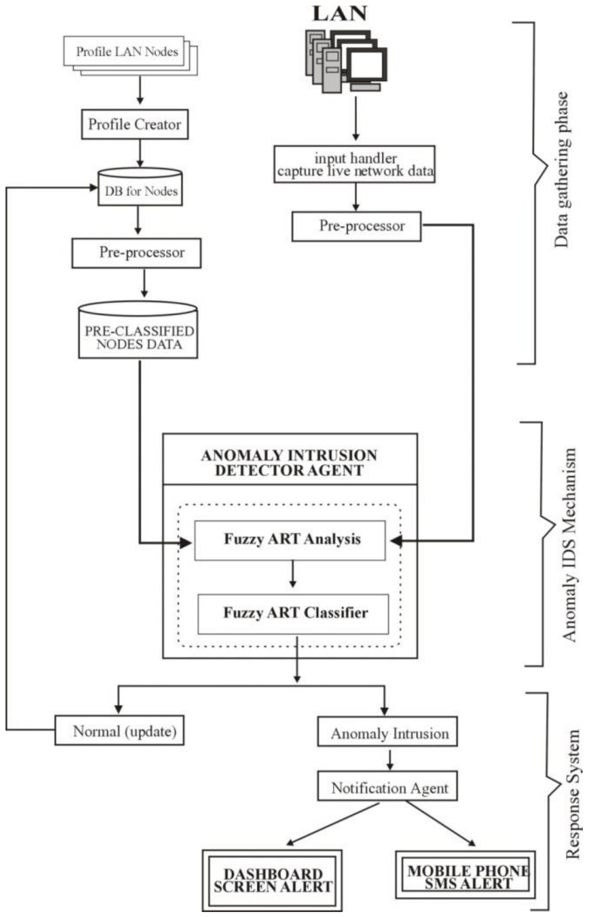

Figure 2: Proposed Anomaly Intrusion Detection System Architecture

Figure 2 shows the system architecture of our proposed anomaly network intrusion detection system. The architecture consists of three major phases which involves the data gathering phase by the network administrator, the detection phase and then the response phase. Each of these phases is further explained below in details.

**Data Gathering Phase**

The data gathering phase involves data collection and profiling. The data collection is done on both the known computers on the network and the unknown computers that might join the network at any given point in time. For the known computers, the network administrator creates a profile for them by capturing the following information about them (node name, ip address, mac address and system name) into the automated system, while the system automatically captures information about the unknown computers or host from the network traffic before moving to the detection phase.

**Detection Phase**

The detection phase or mechanism accepts data from the data gathering phase as input; it analyzes the data patterns and also classifies data into normal or anomaly intrusion using the Fuzzy Adaptive Resonance Theory (F-ART) vigilance and learning rate parameters for profiling and training.

**Response Phase**

The response is part of the network administrator control, and could as well be part of the automatic system update control. The response phase is in-charge of sending the output from the detection mechanism to our proposed network monitoring software solution dashboard / console as screen alert message and also as sms alert message to the network administrator's mobile phone through the notification agent.

## IV PERFORMANCE EVALUATION & DISCUSSIONS

The following are some of the available measures for evaluating intrusion detection system performance [34].

i. True Positive (TP) means the number of connections that were correctly classified as an intrusion.
ii. True Negative (TN) means the number of connections that were incorrectly classified as an intrusion.
iii. False Positive (FP) means the number of intrusion connections that were incorrectly classified as normal.
iv. False Negative (FN) means the number of normal connections that were incorrectly classified as an intrusion.

In evaluating the performance of our anomaly node intrusion detection objective, we mainly concentrated on the Detection Rate (DR), Detection Time (DT), and the false alarm rates.

We used the Fuzzy ART algorithm in analyzing and detecting anomaly intrusion from the network traffic data effectively. Table 2 shows the sample host data that were made to associate with the network without profiling them with our proposed application.

Table 2: Sample data of nodes not profiled on the network

| S/N | IP Address | MAC Address |
|---|---|---|
| 1 | 192.168.1.255 | ff-ff-ff-ff-ff-ff |
| 2 | 224.0.0.2 | 01-00-5e-00-00-02 |
| 3 | 224.0.0.22 | 01-00-5e-00-00-16 |
| 4 | 224.0.0.251 | 01-00-5e-00-00-fb |
| 5 | 224.0.0.252 | 01-00-5e-00-00-fc |
| 6 | 239.255.255.250 | 01-00-5e-7f-ff-fa |
| 7 | 192.168.1.1 | f4-ec-38-ea-13-00 |
| 8 | 192.168.1.2 | 00-0a-41-ba-f9-80 |

(i) The detection rate is computed as follows:

$$\textit{Detection rate (DR)} = \frac{Number\ of\ unprofiled\ system\ detected}{Total\ number\ of\ unprofiled\ systems}\, x\, \frac{100}{1}$$

$$\textit{Detection rate (DR)} = \frac{8}{8}\, x\, \frac{100}{1}$$

*Detection rate (DR)* = 99.99%

All nodes not profiled with our application on the non-production network used in conducting the experiment were detected and logged in our proposed system intrusion log file.

(ii) The detection time result

The system performance in terms of time to detect an anomaly intrusion and the mean time of notifying or reporting the anomaly as screen alert message for the network administrator's consumption is also considered.

We found out that the mean time for our proposed system to report an intrusion in a near real-time situation on the screen is about 0.25 seconds as compared to the mean time of 0.89 seconds recorded by [21], and mean time of 4.42 seconds as recorded by [27]. Here, it should be noted that; the shorter in time (seconds) it takes the detection mechanism to analyze, detect and report intrusion; the better the detection mechanism.

Table 3: Summary of Intrusion detection results

| | Intrusion detection by (Eid, 2004) | Intrusion detection by (Sodiya, 2006) | Our anomaly intrusion detection (2017) |
|---|---|---|---|
| Mean Time | 4.42sec | 0.89sec | 0.25sec |

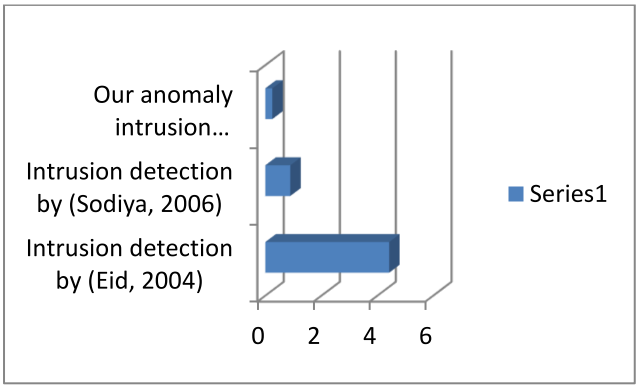

Figure 3: Graphical representation of Table 3

(iii) The false alarm rates result

The system performance in terms of the false alarm rates that can be triggered by our anomaly node intrusion detection mechanism is also discussed. The false positive (FP) and false negative (FN) are considered under this section.

Recall that; false positive (FP) means the number of intrusion connections that were incorrectly classified as normal, while false negative (FN) means the number of normal connections that were incorrectly classified as anomaly intrusion. These concepts are major challenges for any intrusion detection mechanism to handle. Flagging a false report of normalcy when there are actually intrusions on the network or flagging false report of intrusion when the network traffic data is normal but may be with like modification based on the dynamic nature of any network shows that the intrusion detector mechanism may not have been well built or designed.

Again, we considered the concepts of false positive and false negative very seriously in choosing Fuzzy ART technique for designing and building our proposed anomaly intrusion mechanism. We allowed the vigilance and the learning rate parameters to be flexible in order to take care of situations like false positive and false negative occurrence in our developed application. The learning rate parameter ($\beta$) for classifying the network traffic pattern correctly as normal was set to: $39 \leq \beta \leq 49$

Network traffic parameter less than or greater than the learning rate range is also correctly classified as an anomaly intrusion.

Table 4: Sample intrusion data for false positive rate

| | Cases | False Positive Rate |
|---|---|---|
| Intrusion connections | 210 | 0.01% |

Table 5: Sample normal data for false negative rate

| | Cases | False Negative Rate |
|---|---|---|
| Normal connections | 10 | 0.01% |

Table 4 shows that there were cases of 210 intrusion connections to the local area network (LAN), and our proposed anomaly intrusion mechanism correctly detected and classified all of them as intrusion thereby giving a false positive rate of 0.01%, while Table 5 shows cases of 10 normal connections to the LAN. Our application also correctly classified these 10 connections to be normal giving a false negative rate of 0.01%.

## V CONCLUSION

The problem of effective network security is an interesting and challenging one. Several research works on intrusion detection systems were reviewed in order to really address the network security challenges in LAN environment with respect to anomaly node intrusion.

The Fuzzy ART model was proposed in this research work and used to detect anomaly node intrusion in a Local Area Network.

Results revealed that there is a high performance detection rate for our proposed anomaly node intrusion detector on the local area network. Finally, our proposed approach recorded an insignificant level of false alarm rate.

# REFERENCES

[1] Peyman, K. and Ali, A. G. (2005).*Research on Intrusion Detection and Response Survey*, International Journal of Network Security, Vol. 1, No. 2

[2] Vijayarani, S., and Maria, S. S. (2015). *Intrusion Detection System: A Study, International Journal of Security*, Privacy and Trust management (IJSPTM) Vol. 4, No 1.

[3] Amitabh, M., Ketan, N., and Animesh, P. (2004). Intrusion Detection in Wireless Ad Hoc Networks, IEEE Wireless Communications, pp. 48-60.

[4] Karthikeyan, K. R., and Indra, A. (2010). *Intrusion Detection Tools and Techniques: A Survey*, International Journal of Computer Theory and Engineering, Vol. 2, No. 6.

[5] Mukta, G. (2014).*Intrusion Detection System in Campus Network: SNORT-The most powerful Open Source Network Security Tool*, International Journal of Advancement in Engineering Technology, management and Applied Sciences, Vol. 1(5), ISSN: 2349-3224, PP. 1-11

[6] Malik, V., Jhawar, M., Khanijau, A., and Chawla, N. (2014).*LAN Based Intrusion Detection and Alerts*, International Journal of Scientific and Technology Research, Vol 3(5), pp. 229-234

[7] Marinova-Boncheva, V. (2007).*A Short Survey of Intrusion Detection Systems*, Bulgarian Academy of Sciences.

[8] Endorf, C., Schultz, E., and Mellander, J. (2004). Intrusion Detection and Prevention, McGraw-Hill.

[9] Ricardo, P., Maira, H., Javier, G., and Barenco, C. J. (2006). *On the Anomaly Intrusion Detection in Mobile Ad hoc Network Environments*. Personal Wireless Communications, Vol. 4217, Springerlink.

[10] Yongguang, Z., and Wenke, L. (2000).*Intrusion detection in wireless ad-hoc networks*, pp. 275-283, Publication of the Association of Computing Machinery.

[11] Cabrera, J. B. D., Carlos, G., and Raman, M. (2008).*Ensemble Methods for Anomaly Detection and Distributed Intrusion Detection in Mobile Ad-hoc Networks*, Vol. 9(1), pp. 96-119, Elsevier Science Publishers.

[12] Farroq, A. S., and Saswati, S. (2008) Signature based intrusion detection for wireless Ad-hoc Networks: A comparative study of various routing protocols.

[13] Vijay, B., and Ajay, G. (2006).*Anomaly Intrusion Detection in Wireless Sensor Networks*, Journal of High Speed Networks, Vol. 15(1), ACM.

[14] Haiguang, C., Peng, H., Xi, Z., and Chuanshan, G. (2007).*Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks*, Intelligence and Security Informatics, Springlink

[15] Yu, L., Cristina, C., and Hong, M. (2006).*A Bayesian Game Approach for Intrusion Detection in Wireless Ad-hoc Networks*, ACM.

[16] Nakkeeran, R., Aruldoss-Albert, T., and Ezumalai, R. (2010).*Agent Based Efficient Anomaly Intrusion System in Adhoc Networks*. IACSIT International Journal of Engineering and Technology, Vol 2(1), pp. 52-56.

[17] Hongmei, D., Xu, R., Li, J., Zhang, F., Levy, R., and Wenke, L. (2008).*Agent-based cooperative anomaly detection for wireless ad-hoc networks*, Parallel and Distributed Systems, Vol. 1. Pp. 1-8.

[18] Bo, S., Kui, W., Yang, X., and Ruhai, W. (2006).*Integration of mobility and intrusion detection for wireless sensor networks*.

[19] Patil, T. K., and Banchhor, C. O. (2013).*Distributed Innode trusion Detection System using Mobile Agent in LAN Environment*. International Journal of Advanced Research in Computer and Communication Engineering, Vol. 2(4), pp. 1901-1903

[20] Abraham, A., Jain, R., Thomas, J., and Han, S. Y. (2007). D-SCIDS: Distributed soft computing intrusion detection system. Journal of Network and Computer Application, 30, 81-98.

[21] Sodiya, A. S. (2006). *Multi-level and secured agent-based intrusion detection system*. Journal of Computing and Information Technology, 14(3), 217-223.

[22] Singh, M and Sodhi, S. S. (2007) *Distributed Intrusion Detection using Aglet Mobile Agent Technology*, Proceedings of National Conference on Challenges & Opportunities in Information technology, RIMT-IET, MandiGobindgarh

[23] Chaudhary, V. K., and Upadhyay, S. K. (2013) Distributed intrusion detection system using sensor based mobile agent technology, International Journal of Innovations in Engineering and Technology (IJIET), Vol. 3(1), pp. 220-226

[24] Rehak, M., Pechoucek, M., Celeda, P., Novotny, J., and Minarik, P. (2008).*CAMNEP: Agent-Based Network Intrusion Detection System*. In Proceedings of 7th International Conference on Autonomous Agents and Multiagent Systems (AA-MAS), Industry and Applications Track, Berger, Burg, Nishiyama, Estorill, Portugal, pp. 133-136

[25] Chan, P. C., and Wei, V. K. (2002). Preemptive distributed intrusion detection using mobile agents. Proceedings of 11th IEEE International Workshops on Enabling Technologies. pp. 103 – 108.

[26] Wang, H. Q., Wang, Z. Q., Zhao Q., Wang G. F., Zhen g R. J., and Liu, D. X. (2006). *Mobile agents for network intrusion resistance*.APWeb Workshops 2006, LNCS 3842, pp 967-970.

[27] Eid, M., Artail, H., Kayssi, A., and Chehab, A. (2004). An adaptive intrusion detection and defense system based on mobile agents.Proceedings of the Innovations in Information Technologies (IIT'2004), Oct, 2004, Dubai, UA E.

[28] Li, C., Song, Q., and Zhang, C. (2004). *MA-IDS: Architecture for distributed intrusion detection using mobile agents*. Proceedings of the 2nd International Conference on Information Technology for Application (ICITA, 2004)

[29] Deeter, K., Singh, K., Willson, S., Filipozzi, L., and Vuong, S. (2004). *AP HIDS: A mobile agent-based programmable hybrid intrusion detection*. Retrieved from http://www.cc.gatech.edu/grads/k/ksingh/publication/aphids_cameraready.pdf

[30] Barika, F. A., and El - Kadhi, N. (2003). Intelligent and mobile agent for intrusion detection system. Proceedings of International Conference of Information and Communication Technology, Egypt, Nov. 2003.

[31] Kruegel, C., and Toth, T. (2002). Applying mobile agent technology to intrusion detection.Technical Report Number T UV-1841-2002-31, Technical University of Vienna.

[32] Carpenter, G. A., and Grossberg, S. (1991). *Patterns recognition by self-organizing neural networks.*Cambridge, MA: MIT Press.

[33] Jang, J. S., Sun, C. T., and Mizutani, E. (1997). *Neuro-fuzzy and soft computing: A computational approach to learning and machine intelligence*, Englewood Cliffs, NJ: Prentice-Hall.

[34] Onashoga, S. A., Ajayi, O. B., and Akinwale, A. T. (2013).*A Simulated Multiagent-Based Architecture for Intrusion*

*Detection System*.International Journal of Advanced Research in Artificial Intelligence.Vol. 2, No. 4.pp.29 – 38.

## AUTHORS' PROFILE

**John-Otumu Adetokunbo** is currently pursuing Ph.D in Computer Science with specialization in Network security at Ebonyi State University, Abakaliki, Nigeria. He obtained his M.Sc (Info Tech) from National Open University of Nigeria and M.Sc (Computer Science) from Ambrose Alli University, Ekpoma, Nigeria. He is a Senior Technical Officer at the Directorate of Information and Communication Technology, Ambrose Alli University, Ekpoma, Nigeria. He is a member of the Nigeria Computer Society (NCS) and also a Chartered Information Technology Professional registered with the Computer Professionals Registration Council of Nigeria (CPN). His research interest includes Computer communication systems, Agent computing and Multi-agent based systems, Network security, Software engineering and Soft computing. He has published over 15 articles in both local and international Journals.

**E-mail:**macgregor.otumu@gmail.com

**Engr. (Dr.) Ojieabu Clement Eghosa** holds a Ph.D in Communication Engineering, M.Eng in Electronic & Telecommunication Engineering and B.Eng in Electrical/Electronic Engineering. He is an Associate Professor of Communication Engineering at the Department of Electrical/Electronic Engineering, Ambrose Alli University, Ekpoma. He is a registered engineer with the Council for the Regulation of Engineering in Nigeria (COREN). His research interest includes Data communication and security, intelligent systems and satellite communication systems. He has published over 30 articles in both local/international journals and conference proceedings.

**E-mail:**bishopeghosa@yahoo.ca

**Dr. Oshoiribhor Emmanuel Osaze** holds a Ph.D in Computer Science from Ambrose Alli University, Ekpoma, Nigeria, M.Sc., and B.Sc. (Hons) Computer Science from University of Benin, Nigeria. He is a Lecturer in the Department of Computer Science, Ambrose Alli University, Ekpoma, Nigeria. He is a registered member of Nigeria Computer Society (NCS). His research interest includes Data Mining, Artificial Intelligence, and Software Engineering He has published over 16 articles in both local and international Journals.

**E-mail:**emmaoshor2001@gmail.com